

TRORC IT Policy: Email, Internet and File Retention

Purpose

The purpose of this document is to provide summary guidelines regarding internet use, Electronic Mail (email) and Information Technology (IT), at the Two Rivers-Ottawaquechee Regional Commission (TRORC). The TRORC Board and their designees shall review these policies and make changes as necessary. Employees shall read, understand, and adhere to these policies.

TRORC shall provide computer access to all staff and shall provide a variety of electronic information and communications systems for use in carrying out its business. All information and communication transmitted by, received from, or stored in, these systems are the property of TRORC and, as such, are intended to be used for job-related purposes only.

Monitoring

TRORC provides the network, computers, email and, in some instances, other communications devices including cell phones, and tablets, for employee use on company business. TRORC may access any electronic or communications equipment, files, calendars, and emails, and may disclose all data or messages stored or sent on its systems. Employees should not expect any privacy for any communications that touch TRORC infrastructure or TRORC business: computers, wired or wireless networks or email servers. TRORC reserves the right to monitor communication and data at any time, with or without notice. TRORC also reserves the right to disclose the contents of messages for any purpose at its sole discretion.

Retrieval

Notwithstanding TRORC's right to retrieve and read any email and communication messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any email messages that are not specifically sent to them unless authorized by the Executive Director.

Passwords

Passwords shall not be divulged to other staff or persons outside the organization. At no time should a TRORC employee allow a temporary, contractor or another employee the use of their passwords. It is recommended that employees change their passwords regularly. TRORC reserves the right to override any employee-selected passwords. Employees are required to provide IT staff with any passwords to facilitate access as needed. Passwords shall not be stored in unsecured computer data files, on the network, or be displayed openly at any workstations.

Email and Internet protocol

Employees shall exercise good judgment and shall conduct themselves according to existing policies and procedures while using the internet and email. During working hours, employees shall use the internet and email for work purposes. A minimum of personal use of internet access and email is permitted and shall be conducted on the employee's own time. All access to

TRORC IT Policy: Email, Internet and File Retention

internet and email use using TRORC equipment or networks will be subject to the terms of this policy and all information contained within the TRORC email system is owned by TRORC with no confidentiality assumed. Employees that participate in non-work social networking sites should do so on personal time only.

Email message and internet content

The TRORC email and internet systems shall not be used for the following prohibited uses:

- illegal activities
- threats
- harassment
- slander
- defamation
- solicitation or proselytizing for commercial ventures, religious causes, political causes, outside organizations, or other solicitations that are not job related
- advertising or sales of services or merchandise
- outside consulting
- obscene or suggestive messages
- offensive images
- pornographic materials
- chain letters
- private, for-profit commercial activities

Employees should also refrain from using internet and email systems to send jokes, as jokes often contain objectionable material and can be easily misconstrued. In addition, the email and internet systems shall not be used to send or receive copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization from the Executive Director.

Legal Proceedings

Information sent by employees via email may be used in legal proceedings or Freedom of Information Act (FOIA) requests. Emails are considered written communications and may be subject to subpoena in litigation. TRORC may inspect the contents of email messages in the course of an investigation or FOIA and will respond to the legal process and fulfill any legal obligations to third parties.

Email as an official record

Email messages are “official records” if they are made or received in the conduct of TRORC business and shall be treated as formal business documents. Such business includes the provision of services, delivery of programs, development of policies, making of decisions, performance of commission functions, and other similar types of transactions. No emails related and pertinent to TRORC projects, which contain relevant information not otherwise readily available, shall be deleted. Emails may be printed, with the hard-copy retained in consistency

TRORC IT Policy: Email, Internet and File Retention

with record retention policies, and then deleted. Personal or transient emails may be deleted at any time.

Examples of messages sent by e-mail that are records include:

- policies and directives,
- correspondence or memoranda related to official business,
- work schedules and assignments,
- agendas and minutes of meetings,
- drafts of documents that are circulated for comment or approval,
- any document that initiates, authorizes, or completes a business transaction,
- final reports or recommendations

Some examples of messages that *do not constitute records* are:

- personal messages and announcements,
- copies or extracts of documents distributed for convenience or reference,
- phone message slips,
- announcements of social events

Disposition of Public Records

Per 1 V.S.A. §317a, a custodian of public records shall not destroy, give away, sell, discard, or damage any record or records in his or her charge, unless specifically authorized by law or under a record schedule approved by the State Archivist pursuant to 3 V.S.A. §117 (a)(5). “Public record” or “public document” means all papers, documents, machine readable materials, or any other written or recorded matters, regardless of their physical form or characteristics that are produced or acquired in the course of agency business. Individual salaries and benefits of and salary schedules relating to elected or appointed officials and employees of public agencies shall not be exempt from public inspection and copying. “Record schedule” means a manual, directive, or policy containing descriptions of and disposition instructions for retention, access, and management of all public records or public documents.

Email Archiving

TRORC uses a cloud-based Microsoft Exchange Online plan with unlimited archiving for its employees. All emails are moved to the archives after three years.

Back-up Retention

Administrative Support Records

- These files must be kept for at least one year.
- If hard copies are created and filed elsewhere, administrative support records need not be saved.

TRORC IT Policy: Email, Internet and File Retention

Administrative Support Records are those of a general facilitative nature created or received in the course of administering programs. Included are such records as:

- Correspondence of a routine or repetitive type, such as requests for information;
- Inter-office or inter-departmental communications which do not subsequently result in the formulation of policy;
- Reference materials, sometimes of a technical nature, used but not created by the office;
- Daily, weekly, or monthly office activity reports which are summarized in annual reports or which relate to routine activities (including work progress or statistical reports prepared in the office and forwarded to higher levels);
- Personnel data of office that is not duplicated in departmental personnel record;
- Purchase orders, payment vouchers, travel expense statements or similar financial documents that are not duplicated in department/division fiscal office files;
- Daily, weekly, or monthly work assignments (including duty roster files) for office staff;
- Calendars, appointment books, schedules, logs, diaries, and other records documenting meetings, appointments, telephone calls, trips, visits, and other daily activities of employees; and
- Unpublished calendars of events and activities.

Policy and Program Records (Primary Mission Files)

- Policy and Program Records generally need to be retained permanently under specific record schedules and may be transferred to the State Archives at some time during their life cycle.

These records document the formulation and adoption of policies and procedures and the implementation or management of the programs or functions of the office or department. Included are such records as:

- Policies and procedures developed by TRORC that govern the operation of the commission;
- Correspondence with citizens or other government officials regarding policy, procedure development, or program administration;
- Annual, ad hoc, narrative, or statistical reports on program activities, achievements or plans;
- Organizational charts and mission statements;
- Studies regarding TRORC or division operations;
- Circular letters, directives or similar papers addressed to staff or commissioners concerning policies, procedures or programs;
- Records related to significant events in which TRORC participated; and
- Photographs, published material, and other record forms.
- All network resources are backed up weekly to off-site servers.

Personal and Transitory

- Personal and transitory emails should be deleted immediately.

TRORC IT Policy: Email, Internet and File Retention

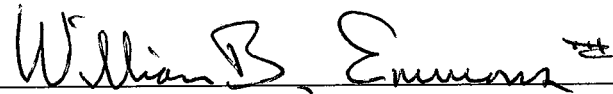
Network and Personal Computer Security

IT staff will monitor network security on a regular basis. IT staff will implement and maintain procedures to provide adequate protection from intrusion in TRORC's computer systems from external sources. Staff shall not store personal, business or other credit card, passwords, or account information within word processing or other data documents.

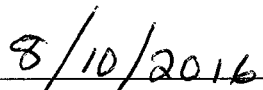
Only legally licensed software shall be installed by IT staff, or by employees with IT staff authorization, on TRORC's computers. Users are expected to read, understand and conform to the license requirements of any software products used or installed. All workstations shall be provided with network threat protection software which shall not be removed or disabled. Employees shall follow these IT policies and shall scan or have scanned incoming communications to their workstations for threats. IT staff will conduct education on opening attachments and other actions designed to enhance security.

The TRORC Executive Director will meet with IT staff on a regular basis and will certify to the TRORC Executive Committee on an annual basis that all aspects of this policy are actively used and understood by all employees.

Adopted by the TRORC Board of Commissioners



TRORC Chair



Date

Employee Acknowledgment

Note: Failure to comply with the TRORC IT and Email policy may result in disciplinary action up to and including legal action and termination of employment. It is the responsibility of the employee to obtain clarification from the Executive Director or IT staff for any portion of this policy that is not understood.

I have read TRORC's IT and Email Policy and agree to abide by it. I understand that violations of this policy may result in discipline, including termination of employment.

Signature

Date

